08-07-00 A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b)

Attorney Docket No. 005129.P001 Total Pages 2

First Named Inventor or Application Identifier David J. Wetherall et al.

Express Mail Label No. EL431686806US

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 29)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 10)

4. X Oath or Declaration (Total Pages 6)

a. X Newly Executed (Original or Copy)

b. ___ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**

i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ___ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ___ Microfiche Computer Program (Appendix)

7. ___ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ___ Computer Readable Copy
b. ___ Paper Copy (identical to computer copy)

(if applicable, all necessary)

a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. _X_ Assignment Papers (cover sheet & documents(s))
9. _____ a. 37 CFR 3.73(b) Statement (where there is an assignee)
_X_ b. Power of Attorney
10. _____ English Translation Document (if applicable)
11. _____ a. Information Disclosure Statement (IDS)/PTO-1449
_____ b. Copies of IDS Citations
12. _____ Preliminary Amendment
13. _X_ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. _X_ a. Small Entity Statement(s)
b. Statement filed in prior application, Status still proper and desired
15. _____ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. _X_ Other: separate sheet with title, express mail label, copy of postcard and attorney's signature

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

___ Continuation ____ Divisional ____ Continuation-in-part (CIP)

of prior application No: __

18. **Correspondence Address**

_____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)

or

_X_ Correspondence Address Below

NAME Aloysius T.C. AuYeung
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard
Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (425) 827-8600 FAX (425) 827-5644

Express Mail Label: EL431686806US

PTO/SB/17(6/99)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL FOR FY 2000

TOTAL AMOUNT OF PAYMENT ($) $634.00

Complete if Known:
Application No. Not Yet Assigned
Filing Date Herewith
First Named Inventor David J. Wetherall et al.
Group Art Unit
Examiner Name
Attorney Docket No. 005129.P001

METHOD OF PAYMENT (check one)

1. [X] **The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:**

Deposit Account Number 02-2666
Deposit Account Name

[X] **Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17**

---

2. X **Payment Enclosed:**
X **Check**
____ **Money Order**
____ **Other**

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility application filing fee	345.00
106	310	206	155	Design application filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional application filing fee	

SUBTOTAL (1) $ 345.00

2. EXTRA CLAIM FEES

		Extra Claims		Fee from below	Fee Paid
Total Claims	39	– 20** =	19	X 9	= 171.00
Independent Claims	5	– 3** =	2	X 39	= 78.00
Multiple Dependent					=

****Or number previously paid, if greater; For Reissues, see below.**

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim, if not paid
109	78	209	39	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) $ 249.00

FEE CALCULATION (continued)

Patent fees are subject to annual revisions. Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid.
See Forms PTO/SB/09-12

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	380	216	190	Extension for response within second month	
117	870	217	435	Extension for response within third month	
118	1,360	218	680	Extension for response within fourth month	
128	1,850	228	925	Extension for response within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive unavoidably abandoned application	
141	1,210	241	605	Petition to revive unintentionally abandoned application	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	760	246	380	For filing a submission after final rejection (see 37 CFR 1.129(a))	
149	760	249	380	For each additional invention to be examined (see 37 CFR 1.129(a))	
Other fee (specify)					
Other fee (specify)					

SUBTOTAL (3) $ 40.00

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:

Typed or Printed Name: Aloysius T.C. AuYeung

Signature _____ **Date** 8/4/2000

Reg. Number 35,432 **Deposit Account User ID** _____ (complete if applicable)

Inventors: David J. Wetherall, et al. Attorney's
Serial or Patent No.: not yet assigned Docket No. 005129.P001
Filed or Issued: herewith
For: A DISTRIBUTED SOLUTION FOR REGULATING NETWORK TRAFFIC

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
37 CFR 1.9 (f) and 1.27(c) - - SMALL BUSINESS CONCERN

I hereby declare that I am:

[____] the owner of the small business concern identified below:
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN: Asta Networks, Inc.
ADDRESS OF CONCERN: 1100 EASTLAKE, SUITE 200, SEATTLE, WA 98109

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby certify that to the best of my knowledge and belief rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention entitled A DISTRIBUTED SOLUTION FOR REGULATING NETWORK TRAFFIC by inventor(s) David J. Wetherall, Tom Anderson, Stefan Savage described in

[X] the specification being filed herewith
[____] application serial no. _____, filed _____
[____] patent no. _____, issued _____

and I have reviewed the document that evidences the conveyance of those rights. That document

[X] is being filed herewith.
[____] was recorded in the Patent and Trademark Office on _____, 19__ at reel _____ and frame _____.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed below and **no rights to the invention are held by any person, other than the inventor, who could not qualify as a small business concern under 37 CFR 1.9(d) or by any concern which would not qualify as a small business concern under 347 CFR 1.9(d) or a non-profit organization under 37 CFR 1.9(e)**. NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME: _____

ADDRESS: _____

[____] Individual [_____] Small Business Concern [_____] Non-Profit Organization

NAME: _____

ADDRESS: _____

[____] Individual [_____] Small Business Concern [_____] Non-Profit Organization

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: Andrew Konstantaras

TITLE OF PERSON OTHER THAN OWNER: VICE PRESIDENT MARKETING

ADDRESS OF PERSON SIGNING: 1100 EASTLAKE, SUITE 200, SEATTLE, WA 98109

SIGNATURE: _____ DATE: 8/4/00

Our Ref.: 005129.P001

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

A Distributed Solution for Regulating Network Traffic

Inventor(s):
David J. Wetherall
Thomas E. Anderson
Stefan R. Savage

Prepared by:
Blakely, Sokoloff, Taylor & Zafman, LLP
Seattle/Kirkland Office

"Express Mail" label number: EL431686806US

A Distributed Solution for Regulating Network Traffic

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of networking. More specifically, the present invention relates to the regulation of network traffic.

2. Background Information

With advances in integrated circuit, microprocessor, networking and communication technologies, increasing number of devices, in particular, digital computing devices, are being networked together. Devices are often first coupled to a local area network, such as an Ethernet based office/home network. In turn the local area networks are interconnected together through wide area networks, such as ATM networks, Frame Relays, and the like. Of particular notoriety is the TCP/IP based global inter-networks, Internet.

As a result this trend of increased connectivity, increasing number of applications that are network dependent are being deployed. Examples of these network dependent applications include but are not limited to, email, net-based telephony, world wide web and various types of e-commerce. For these applications, success inherently means high volume of desirable network traffic for their implementing servers. To ensure continuing success, quality of service through orderly and efficient handling of the large volume of network traffic has become of paramount importance. Various subject matters, such as scalability, distributive deployment and caching of contents as well as regulating network traffic destined for a network node have become of great interest to the artesian.

SUMMARY OF THE INVENTION

The present invention provides for a method and apparatus for controlling the amount and/or type of network traffic destined to cross a network link, such as a router, to facilitate ensuring the quality of service provided by the network nodes attached to such network link. The present invention may be used to shape the volume and/or the type of network traffic arriving at a network node or network traffic in or near the neighborhood of the network node, to help ensure quality of service provided by the network node. The present invention may also be used to block, in whole or in part, network traffic, thereby protecting the network node in or near the path of such traffic from denial of service attacks.

A number of sensors are distributively deployed in the network. The sensors are either integrally disposed in a number of routing devices of the network or externally disposed and coupled to the routing devices. The sensors monitor and report on network traffic routed through the routing devices. A director is also provided to receive network traffic reports from the sensors for the routing devices, and to determine whether moderating actions are to be taken to moderate an amount of network traffic destined for at least one of a number of network nodes of the network, based at least in part on some of the network traffic reports received from the sensors. In one embodiment, upon determining moderating actions are to be taken, the director further determines the moderating actions to be taken, including where the moderating actions are to be taken. In one embodiment, the director further instructs appropriate ones of the sensors to cause the desired

moderating actions to be applied on the network traffic going through some of the routing devices.

In one embodiment, the director, in cooperation with the sensors, also determines when and where moderating actions are to be relaxed, and causes such relaxation to be effectuated. In yet another embodiment, the director, in cooperation with the sensors, also determines when and where regulating actions filtering out certain types of network traffic destined for a network node are to be applied, and causes such filtering to be performed.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates a network view of the present invention, including a number of distributively deployed sensors and a director, in accordance with one embodiment;

Figure 2 illustrates a method view of the same invention, in accordance with one embodiment;

Figure 3 illustrates a functional view of a sensor, in accordance with one embodiment;

Figures 4-6 illustrate the operational flow of the relevant aspects of the requestor, reporter and command generation functions of **Fig. 3**, in accordance with one embodiment each;

Figure 7 illustrates an architectural view of a sensor, in accordance with one embodiment;

Figure 8 illustrates a functional view of a director, in accordance with one embodiment;

Figures 9-11 illustrate the operational flow of the relevant aspects of the send/receive, analyzer and regulator functions of **Fig. 8**, in accordance with one embodiment each; and

Figure 12 illustrates an example computer system suitable for use to host a software implementation of a sensor or the director, in accordance with one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Parts of the description will be presented in terms of operations performed by a processor based device, using terms such as requesting, reporting, determining, data, and the like, consistent with the manner commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. As well

understood by those skilled in the art, the quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, and otherwise manipulated through mechanical and electrical components of the processor based device; and the term processor include microprocessors, micro-controllers, digital signal processors, and the like, that are standalone, adjunct or embedded.

Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations need not be performed in the order of presentation. The terms "routing device", and "route" are used throughout this application, in the claims as well as in the specification. The terms as used herein are intended to have a broader meaning than its normal plain meaning as understood by those ordinarily skilled in the networking art. They are intended to be genus terms that include the conventional routers and conventional routing and forwarding, as well as all other variations of network trafficking, such as, switches or switching, gateways, hubs and the like. Thus, unless particularized, the terms are to be given this broader meaning. Further, the description repeatedly uses the phrase "in one embodiment", which ordinarily does not refer to the same embodiment, although it may.

Overview

Referring now first to **Figures 1-2**, wherein two block diagrams illustrating a network view and a method view of the present invention, in accordance with one embodiment, are shown. As illustrated in **Fig 1**, in accordance with the present invention, a number of distributively disposed sensors, such as sensors **104a-104c**,

are provided to monitor and report on network traffic routed through routing devices of network **100**, such as routing devices **106a-106c**, for various network nodes, such as clients **108a-108b** and server **110**. Further, director **102** is provided to determine whether regulatory actions are to be taken to regulate an amount of network traffic destined for a network node, such as server **110**, to ensure quality of service provided by the network node. Director **102** advantageously makes the determination automatically, based at least in part on the network traffic data reported by the sensors.

Further, director **102** advantageously determines the nature of the regulatory action, including where the regulatory actions are to be taken. As will be explained in more detail below, in a preferred embodiment, the regulatory actions are advantageously administered at locations away from the network node itself. Director **102** also determines at a subsequent point in time whether to relax the regulatory actions. In like manner, director **102** also determines the amount of relaxation and which regulated locations are to be partially or completely de-regulated.

Network **100** is intended to represent a broad range of private as well as public networks or interconnected networks, such as the network of an Internet Service Provider (ISP), the enterprise network of a multi-national corporation, or the Internet.

Networking nodes, such as clients **108a-108b** and server **110** are coupled to each other through routing devices **106a-106c** and networking fabric **112**. As disclosed earlier, routing devices **106a-106c** are intended to represent a broad range of network trafficking equipment, including but not limited to conventional routers, switches, gateways, hubs and the like. Networking fabric **112** is intended to

represent a broad range of interconnected local as well as wide area networks, formed with the aforementioned and other networking equipment known in the art.

For the illustrated embodiment, sensors **104a-104c** are externally disposed and correspondingly coupled to routing devices **106a-106c**. In a preferred embodiment, sensors **104a-104c** are proximately disposed to routing devices **106a-106c** situated at the boundary entry points of different domains of the network. For example, in the case of the Internet, sensors **104a-104c** are advantageously disposed "adjacent" to routing devices located at the "points of presence" of the Internet, including those "points of presence" where networks peer (exchange traffic) with one another, and where networks connect to their customers.

In alternate embodiments, each sensor **104a**, **104b** or **104c** may monitor and report on the network traffic routed through more than one router, as opposed to the corresponding configuration illustrated for ease of understanding. In yet other embodiments, some or all of sensors **104a-104c** may be integrally disposed within routing devices **106a-106c** instead. Sensors **104a-104c**, whether externally disposed or integrally disposed, are additionally coupled to director **102**. The coupling may be made using any one of a number of communication links known in the art, such as modem links over conventional phone lines, serial communication lines, parallel communication lines, Digital Subscriber Lines (DSL), Integrated Service Digital Network (ISDN) connections, Asynchronous Transfer Mode (ASM) links, Frame Relay connections, Ethernet, IP networks, packet-switched wireless networks, and the like.

While for ease of understanding, only one director **102**, and a handful each of network nodes, clients **108a-108b** and server **110**, routing devices **106a-106c** and sensors **104a-104c** are included in the illustration, from the description to follow, those skilled in the art will appreciate that the present invention may be practiced

with more than one director (or director device) **102** as well as more or less network nodes, routing devices **106a-106c** and sensors **104a-104c**. If more than one director/director device **102** is employed, each director/director device **102** may be assigned responsibility for a subset of sensors **104a-104c**, and the directors may relate to each other in a master/slave relationship, with one of the directors serving as the "master" (and the others as "slave"), or as peers to one another or organized into an hierarchy.

As illustrated in more details in **Figure 2**, in accordance with the present invention, distributively disposed sensors **104a-104c** monitor and report on network traffic routed through routing devices **106a-106c**, block **202**. The reporting may be self-initiated or provided in response to a request. In one embodiment, the reported data include various statistics describing the network traffic that is forwarded. In one embodiment, the reported data may include destination information, allowing the amount of network traffic destined for various network nodes of interest be discernable; volume of data with specific destinations passing through a routing device; volume of data from specific source addresses passing through a routing device; volume of data with specific source and destination address combinations, the types of traffic passing through a routing device; and characteristics of packets of data. Examples of "traffic type" include Web, DNS, Real Networks, Secure Web, Other TCP, Other UDP, ICMP, TCP packets with ACK set, TCP packets without SYN set, and so forth. Examples of "characteristics" include distribution of lengths of packet, distribution of Time To Live values, and so forth.

At block **206**, in response to the receipt of the reported data, director **102** automatically determines whether arrival of network traffic at a network node of interest needs to be regulated or de-regulated. The network nodes of interest may

be provided to director **102** statically or dynamically (including additions as well as subtractions) in any one of a number of techniques known in the art.

In its simplest form, regulation may mean moderating the arrival rate of network traffic destined for a network node of interest. However, regulation may also mean moderating the arrival of particular types and/or characteristics of network traffic. At its extreme, regulation could include completely blocking off network traffic destined for the network node of interest. Similarly, de-regulation means relaxing the amount of moderation being applied to the network traffic destined for the network node of interest, in terms of volume, type, characteristics and so forth. In its most fundamental form, de-regulation could simply involve removal of existing regulations in effect for network traffic destined for the network node of interest.

At block **208**, director **102** determines and/or selects the locations to administer the regulation/de-regulation. In one embodiment, boundary entry locations with the largest volume of network traffic destined for the network node are selected for regulation, and boundary entry locations with the most stringent regulations are selected for de-regulation. At **210**, director **102** also determines the regulation/de-regulation actions. Examples of moderating actions include but are not limited to limiting the bandwidth available for, lowering the priority, or altering the route of network traffic destined for the network node of interest (including perhaps changing their destinations). Accordingly, examples of moderation relaxation actions include but are not limited to their "inverses", i.e. expanding the bandwidth available for, increasing the priority, reconfiguring to potentially shorter routes of network traffic destined for the network node of interest. Similarly, examples of blocking actions include but are not limited to filtering out network traffic destined for the network node of interest, and examples of unblocking actions include but are not

limited to cessation of filtering of the network traffic destined for the network node of interest.

Those skilled in the art will appreciate that the present invention is a superior approach to the prior art approach of regulating network traffic at the network node of interest, using e.g. a firewall. By regulating/de-regulating at remote locations, the present invention advantageously allows the regulation/de-regulation to be administered in a substantially source oriented manner, that is at locations close to the sources of the network traffic (even though the sources often time can not be precisely determined). Further, the remote regulation/regulation lightens the workload at the network node of interest, and allows the bandwidth and resources of the network node be fully available and dedicated to servicing the arrived network traffic.

At block **210**, director **102** issues the regulation/de-regulation instructions to the responsible ones of sensors **104a-104c**, for the locations to be regulated/de-regulated, with respect to network traffics destined for the network nodes of interests. At block **212**, instructed ones of sensors **104a-104c** cause the desired regulation/de-regulation actions to be applied to their corresponding routing devices **106a-106c** to effectuate the desired regulation/de-regulation of the network traffic for the particular nodes of interest. Sensors may also report on traffics impacted by the imposed regulations.

Sensors

Figure 3 illustrates a functional view of a sensor, in accordance with one embodiment. The embodiment assumes the sensor is externally disposed, outside of its responsible router or routing devices. As illustrated, sensor **104a**, **104b** or **104c** includes requestor function **302**, reporter function **304** and command

generation function **306** operatively coupled to each other as shown. Requestor function **302** is used to request a router or routing devices for data depicting network traffic routed through the routing device(s). The request/requests may be made periodically, on demand or in response to some event. The request/requests may be made using any one of a number of communication protocols known in the art. As alluded to, examples of such data are network traffic statistical data, and preferentially, the data include destination information of the network traffic routed. Requestor **302** is also used to request a routing device(s) to alter its/their routing operations to effectuate a desired regulation/de-regulation on the routing device(s), with respect to network traffic going through the routing device(s). The routing operation altering request commands are typically made as a result of regulation/de-regulation instructions provided by director **102**. Similarly, the commands may be provided to the routing device(s) via any one of a number of communication protocols known in the art.

Reporter function **304** is used to report the gathered network traffic data. More specifically, reporter function **304** reports the gathered network traffic data to director **102**. The report may be made periodically, on demand, or in response to some event, such as the occurrence of some pre-specified traffic condition. The report may be made in any one of a number of formats, via any one of a number of communication protocols known in the art.

Command generation function **306** generates the specific commands for the routing device(s) that is responsive to the regulation/de-regulation instructions received from director **102**.

Figures 4-6 illustrate the operation flow of the relevant aspects of request function **302**, report function **304** and command generation function **306**, in accordance with one embodiment each. For request function **302**, as illustrated in

fig. 4, upon start up, it awaits expiration of a timer, block **402**. The periodicity of expiration is application dependent. Upon expiration of the timer, at block **404**, request function **302** requests its responsible routing device(s) for network traffic data. The request may be for all network nodes, for particular network nodes of interest or some other subset of network traffic. At blocks **406** and **408**, request function **302** accumulates and saves the network traffic data provided. Upon completion of the data transfer, requestor function **302** returns to block **402**. However, if timer has not expired, block **402**, request function **302** determines if any regulation/de-regulation commands are to be sent to its responsible routing device(s), block **410**. If there are commands queued awaiting transmission to the routing device(s), request function **302** dequeues and sends the commands to the routing device(s) accordingly, block **412**. Upon sending the commands, request function **302** returns again to block **402**.

For report function **304**, as illustrated in **fig. 5**, in like manner, upon start up, it awaits for the expiration of a timer, block **502**. Likewise, the periodicity of expiration is application dependent. Upon expiration, i.e. time for reporting, report function **304**, takes the most recently received and saved network traffic data, and sends them to director **102**, as earlier described, blocks **504-506**. Upon transmission, report function **304** returns to block **502**.

For command generation function **306**, as illustrated in **fig. 6**, upon start up, it awaits for regulation/de-regulation instructions from director **102**, block **602**. Upon receipt of regulation/de-regulation instructions, command generation function **306** generates the appropriate commands for the particular routing device(s) the sensor is responsible, and queues the commands for transmission to the routing device(s), as alluded to earlier. Upon generating and queuing the appropriate commands,

function **306** returns to block **602** to await additional regulation/de-regulation instructions from director **102**.

Figure 7 illustrates an architectural view of a sensor, in accordance with a hardware/firmware implementation. As illustrated, sensor **700** includes processor **702**, non-volatile memory **704**, LAN and WAN interfaces **706** and **708**. Processor **702** and non-volatile memory **704** are intended to represent a broad range of these elements known in the art. In the case of processor **702**, it may be any 8-bit/16-bit micro-controllers, or 16-bit/32-bit digital signal processors, or even more powerful general purpose microprocessors known in the art. Non-volatile memory **704** may be EEPROM, Flash memory or other memory of the like. Non-volatile memory **704** is employed to store the firmware implementing the earlier described request, report and command generation functions of sensor **700**, and for the embodiment, facilitates these functions execution in place. LAN interface **706** may be an Ethernet, Token Ring or other LAN interfaces of like kind, and WAN interface **708** may be a modem, or an ISDN adapter and the like.

In an alternate embodiment, request, report and command generation functions **302-306** of **Fig. 3**, may be implemented in software via high level languages such as C, and the software implementation may be hosted by a computing device near its responsible routing device(s), provided the hosting computing device is properly equipped with the appropriate communication interfaces to communicate with its responsible routing device(s), and director **102**.

In yet other embodiments, as alluded to earlier, request, report and command generation functions **302-306** of **Fig. 3**, may be incorporated as an integral part of its responsible router. In these embodiments, instead of gathering the network traffic data via request/reply transaction conducted over a communication protocol,

request function **302** may gather the network traffic data through bus transactions, such as direct memory access (DMA) operations accessing the appropriate internal storage units of the router for the collected data. Similarly, in lieu of generating commands designed for a command interface, command generation functions may directly invoke the applicable router routines to cause the routing operation alteration to be effectuated instead.

Director

Referring now to **fig. 8**, wherein a functional view of the director, in accordance with one embodiment is shown. As illustrated, director **102** includes send/receive function **802**, analyzer **804**, and regulator **806**, operatively coupled to each other as shown. Send/receive function **802** is employed to receive network traffic data reported by the distributively disposed sensors, and to send regulation/de-regulation instructions to the distributively disposed sensors. Analyzer **804** analyzes the network traffic data to determine if regulation/de-regulation actions need to be taken, and alerts regulator **806** accordingly. In one embodiment, analyzer **804** determines if regulation/de-regulation actions need to be taken based on whether the volume of traffic has reached a moderating/filtering threshold (in the case of regulation), or fell below a relaxation threshold (in the case of de-regulation). Regulator **806** is used to determine the location or locations of regulation/de-regulation, and what the regulation/de-regulation actions should be. In one embodiment, boundary entry points with the largest amount of network traffic destined for a network node of interest are selected for regulation, whereas the most regulated boundary entry points are selected for de-regulation. In another embodiment, boundary entry points with above threshold level of certain "undesirable" network traffic destined for a network node of interest are selected for

regulation, whereas regulated boundary entry points with below threshold level of the "undesirable" network traffic are selected for de-regulation. Threshold level may simply be the presence of any of such traffic. As described earlier, "undesirable" may be any volume, type and/or characteristic of network traffic.

Figures 9-10 illustrate the operational flow of the relevant aspects of the send/receive, analyzer and regulation functions **802-806**, in accordance with one embodiment each. As illustrated in **Fig. 9**, for the send/receive function, upon start up, it determines if there are network traffic data to be received from the sensors, block **902**. If there are, send/receive function **802** receives the network traffic data being reported accordingly. If there are not, send/receive function **802** determines if there are regulation/de-regulation instructions to be sent to the sensors. If there are, send/receive function **802** sends the regulation/regulation instructions accordingly. If there are not, send/receive function **802** returns to block **902** to determine if there are data to be received again.

As illustrated in **fig. 10**, upon start up, analyzer **804** determines if there are network nodes to be analyzed, block **1002** or some other instruction requiring analysis of network traffic. If there are not, it awaits for the "enrollment" of a network node of interest or some other pre-defined event or state. If there are, analyzer **804** selects a network node to be monitored, block **1004**. Analyzer **804** further determines if regulations are being administered on behalf of the network node, block **1006**. If network traffic is being regulated, analyzer **804** further determines if the network traffic has fallen below the de-regulation threshold or thresholds, **1008**. If the network traffic has not fallen below the de-regulation threshold/thresholds, no actions are taken. If the network traffic has fallen below the de-regulation threshold/thresholds, analyzer **804** notifies/alerts regulator **806** accordingly, block

1012. Back at block **1006**, if regulation is not in progress, analyzer **1010** determines if the network traffic has reached a regulation threshold or thresholds, **1008**. If the network traffic has not reached or surpassed the regulation threshold/thresholds, no actions are taken. If the network traffic has reached or surpassed the regulation threshold/thresholds, analyzer **804** notifies/alerts regulator **806** accordingly, block **1012**.

As illustrated in **fig. 11**, upon receipt of an alert, regulator **806** determines if the alert is for regulation or de-regulation, block **1102**. If the alert is for regulation, regulator **806** selects the boundary entry points for regulation, **1106**. Further, regulator **806** also determines the level of regulation, e.g. how much bandwidth to reduce, or how many priority levels to drop, block **1108**. Upon making these determinations, regulator **806** provides the appropriate sensors with the regulation/de-regulation instructions accordingly, block **1114**. On the other hand, if the alert is for de-regulation, regulator **806** selects the most regulated boundary entry points for de-regulation, **1110**. Further, regulator **806** determines the level of de-regulation, e.g. how much bandwidth to increase, or how many priority levels to bump up, block **1112**. Upon making these determinations, regulator **806** provides the appropriate sensors with the regulation/de-regulation instructions accordingly, block **1114**.

Example Host Computer System

Figure 12 illustrates an example computer system suitable for use as either a host to a software implementation of a sensor, or the director in accordance with one embodiment. As shown, computer system **1200** includes one or more processors **1202** (typically depending on whether it is used as host to sensor or the director), and system memory **1204**. Additionally, computer system **1200** includes

mass storage devices **1206** (such as diskette, hard drive, CDROM and so forth), input/output devices **1208** (such as keyboard, cursor control and so forth) and communication interfaces **1210** (such as network interface cards, modems and so forth). The elements are coupled to each other via system bus **1212**, which represents one or more buses. In the case of multiple buses, they are bridged by one or more bus bridges (not shown). Each of these elements perform its conventional functions known in the art. In particular, system memory **1204** and mass storage **1206** are employed to store a working copy and a permanent copy of the programming instructions implementing the teachings of the present invention. The permanent copy of the programming instructions may be loaded into mass storage **1206** in the factory, or in the field, as described earlier, through a distribution medium (not shown) or through communication interface **1210** (from a distribution server (not shown). The constitution of these elements **1202-1212** are known, and accordingly will not be further described.

Conclusion and Epilogue

Thus, it can be seen from the above descriptions, a novel method and apparatus for regulating network traffic using a distributed approach has been described. The novel scheme enables the quality of service provided by a network node to be ensured, including nullification of denial of service attacks.

While the present invention has been described in terms of the above illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims. For examples, as alluded to earlier, the present invention may be practiced with more or

less sensors, more directors, and so forth. Thus, the description is thus to be regarded as illustrative instead of restrictive on the present invention.

CLAIMS

What is claimed is:

1. A network comprising:

a plurality of network nodes;

a plurality of routing devices to route network traffics between selected ones of said network nodes;

a plurality of sensors, either integrally disposed in a subset of said routing devices or externally disposed and coupled to the subset of routing devices, to monitor and report on network traffic routed through the subset of routing devices; and

a director coupled to said sensors to receive network traffic information from said sensors for said subset of routing devices, and to determine in response whether moderating actions are to be taken to moderate an amount of network traffic destined for at least one of said network nodes, based at least in part on some of said network traffic information received from said sensors.

2. The network of claim 1, wherein the sensors are equipped to periodically gather data denoting at least amount of network traffic routed through said subset of routing devices, said data including destinations of said network traffic.

3. The network of claim 1, wherein the sensors are equipped to periodically report to said director data denoting at least amount of network traffic routed through said subset of routing devices, said data including destinations of said network traffic.

4. The network of claim 1, wherein the sensors are equipped to facilitate application of desired moderation on network traffic through selected ones of said subset of routing devices.

5. The network of claim 1, wherein the director is further employed to determine in response moderating actions to be taken, including where the moderating actions are to be taken, if the director determines that moderating actions are to be taken to moderate the amount of network traffic.

6. The network of claim 1, wherein the director is further employed to determine in response whether moderating actions are to be relaxed for the at least one of the network nodes, based at least in part on some of said network traffic reports received from said sensors.

7. The network of claim 6, wherein the director is further employed to determine in response moderation relaxation actions to be taken, including where the moderation relaxation actions are to be taken, if the director determines that moderation relaxation actions are to be taken to relax moderation on the amount of network traffic.

8. The network of claim 1, wherein the director is further employed to determine in response whether filtering actions are to be taken for the at least one of the network nodes, based at least in part on some of said network traffic reports received from said sensors.

9. The network of claim 8, wherein the director is further employed to determine in response where the filtering actions are to be taken, if the director determines that filtering actions are to be taken to filter out network traffic.

10. The network of claim 8, wherein the sensors are equipped to facilitate application of desired filtering on network traffic through selected ones of said subset of routing devices.

11. The network of claim 1, wherein the director comprises a plurality of director devices corresponding to a plurality of network domains to facilitate said receipt of information on network traffic from sensors in the corresponding network domains, and to incorporate the network traffic information of the different domains in said determination of moderating actions.

12. A method comprising:

routing network traffic to and from a plurality of network nodes of a network;

monitoring and reporting on a portion of said network traffic routed through a plurality of routing devices distributively disposed in the network; and

determining whether moderating actions are to be taken to moderate an amount of network traffic destined for at least one of said network nodes, based at least in part on some of said network traffic reports received for said routing devices.

13. The method of claim12, wherein said monitoring comprises periodically gathering data denoting network traffic routed through said routing devices, said data including destinations of said portion of network traffic.

14. The method of claim 12, wherein said reporting comprises periodically reporting on data denoting said portion of network traffic routed through said routing devices, said data including destinations of said portion of network traffic.

15. The method of claim 12, wherein said method further comprises facilitating application of desired moderation on network traffic passing through selecting ones of said routing devices.

16. The method of claim 12, wherein said method further comprises determining moderating actions to be taken, including where the moderating actions are to be taken, if it is determined that moderating actions are to be taken to moderate the amount of network traffic destined for a network node.

17. The method of claim 12, wherein the method further comprises determining in response whether moderating actions are to be relaxed for the at least one of the network nodes, based at least in part on some of said network traffic reports received from said sensors.

18. The method of claim 17, wherein the method further comprises determining in response moderation relaxation actions to be taken, including where the moderation relaxation actions are to be taken, if it is determined that moderation relaxation actions are to be taken to relax moderation on the amount of network traffic destined for a network node.

19. The method of claim 12, wherein the method further comprises determining in response whether filtering actions are to be taken for the at least one of the network

nodes, based at least in part on some of said network traffic reports received from said sensors.

20. The method of claim 19, wherein the method further comprises determining in response where the filtering actions are to be taken, if it is determined that filtering actions are to be taken to filter out network traffic destined for a network node.

21. The method of claim 19, wherein the method further comprises facilitating application of desired filtering on network traffic through selected ones of said subset of routing devices.

22. The method of claim 12, wherein said sensing is performed using a collection of hierarchically organized devices.

23. The method of claim 12, wherein said determining is performed using a collection of hierarchically organized devices.

24. An apparatus comprising:

(a) a storage medium having stored therein a plurality of programming instructions designed to implement (a.1) a requestor to request a routing device of a network for data denoting network traffic routed through saidrouting device, and to request alteration of routing operations of said routing device to moderate an amount of network traffic going through said routing device, (a.2) a reporter to report said data denoting network traffic routed through saidrouting device, and (a.3) a regulator to control submission of said network traffic moderation routing operation alteration requests to saidrouting device, responsive to moderation instructions provided; and

(b) a processor coupled the storage medium to execute the programming instructions.

25. The apparatus of claim 24, wherein the apparatus further comprises a communication interface coupled to the processor, to couple the apparatus to said routing device and to facilitate submission of said network traffic moderation routing operation alteration requests to saidrouting device.

26. The apparatus of claim 24, wherein the apparatus further comprises a communication interface coupled to the processor, to couple said apparatus to a director that determines whether moderate actions are to be taken to moderate an amount of network traffic, based on said data reported, to facilitate reporting of said data to said director.

27. The apparatus of claim 26, wherein the apparatus further comprises a communication interface to couple the apparatus to at least one of a plurality of hierarchically organized director devices coupled to each other to facilitate data collection, analysis and traffic regulation.

28. The apparatus of claim24, wherein the requestor is further used to request alteration of routing operations of said routing device to relax moderate an amount of network traffic going through said routing device.

29. The apparatus of claim24, wherein the requestor is further used to request filtering operations of said routing device to filter out network traffic going through said routing device.

30. A networking apparatus comprising:

a first functional unit to route network traffic;

a second functional unit coupled to the first functional unit to gather data denoting network traffic routed through arouting device, and to apply moderating actions to said first functional unit to moderate network traffic going through said networking apparatus;

a third functional unit coupled to the second functional unit to report said data; and

a fourth functional unit coupled to the second functional unit to control application of said moderating actions to said first functional unit to effectuate a desired moderation of network traffic going through said networking apparatus , responsive to moderation instructions provided.

31. The networking apparatus of claim 30, wherein the networking apparatus further comprises a communication interface coupled to the fourth functional unit, to couple said networking apparatus to a director that determines whether moderate actions are to be taken to moderate an amount of network traffic, based on said data reported, to facilitate reporting of said gathered data to said director.

32. The networking apparatus of claim 30, wherein the second functional unit is further used to relax moderating actions applied to the first functional unit to relax moderating an amount of network traffic going through said routing device.

33. The networking apparatus of claim30, wherein the second functional unit is further used to cause the first functional unit to filter out network traffic going through said networking apparatus.

34. An apparatus comprising:

(a) a storage medium having stored therein a plurality of programming instructions designed to implement a director to receive reporting of data denoting network traffic routed through a plurality of routing devices of a network, and to determine in response whether moderating actions are to be taken to moderate an amount of network traffic destined for at least one of a plurality of network nodes of said network, based at least in part on some of said reported data; and

(b) a processor coupled the storage medium to execute the programming instructions.

35. The apparatus of claim34, wherein said programming instructions are designed to determine whether a moderation threshold has been reached for a network node, based at least in part on some of said reported data.

36. The apparatus of claim35, wherein said programming instructions are further designed to determine moderating actions to be taken, including where the moderating actions are to be taken, if it is determined that moderating actions are to be taken to moderate an amount of network traffic.

37. The apparatus of claim 34, wherein the apparatus further comprises a communication interface coupled to the processor, to couple the apparatus to a plurality of sensors to receive said data reporting.

38. The apparatus of claim34, wherein the director further determines whether moderating actions being applied are to be relaxed, based at least in part on some of said reported data.

39. The apparatus of claim 34, wherein the director further determines whether filtering actions are to be taken to filter out network traffic, based at least in part on some of said reported data.

ABSTRACT OF THE DISCLOSURE

A number of sensors are distributively deployed in a network, either integrally disposed in a number of routing devices of the network or externally disposed and coupled to the routing devices, to monitor and report on network traffic routed through the routing devices. A director is provided to receive network traffic reports from the sensors for the routing devices, and to determine whether moderating actions are to be taken to moderate an amount of network traffic, based at least in part on some of the network traffic reports received from the sensors. In one embodiment, upon determining moderating actions are to be taken, the director further determines what kind of moderating actions are to be taken, including where the moderating actions are to be taken. In one embodiment, the director further instructs appropriate ones of the sensors to cause the desired moderating actions to be applied on the network traffic going through some of the routing devices. In one embodiment, the director, in cooperation with the sensors, also determines when and where moderating actions are to be relaxed, and causes such relaxation to be effectuated. In yet another embodiment, the director, in cooperation with the sensors, also determines when and where regulating actions filtering out certain types of network traffic destined for a network node are to be applied, and causes such filtering to be performed.

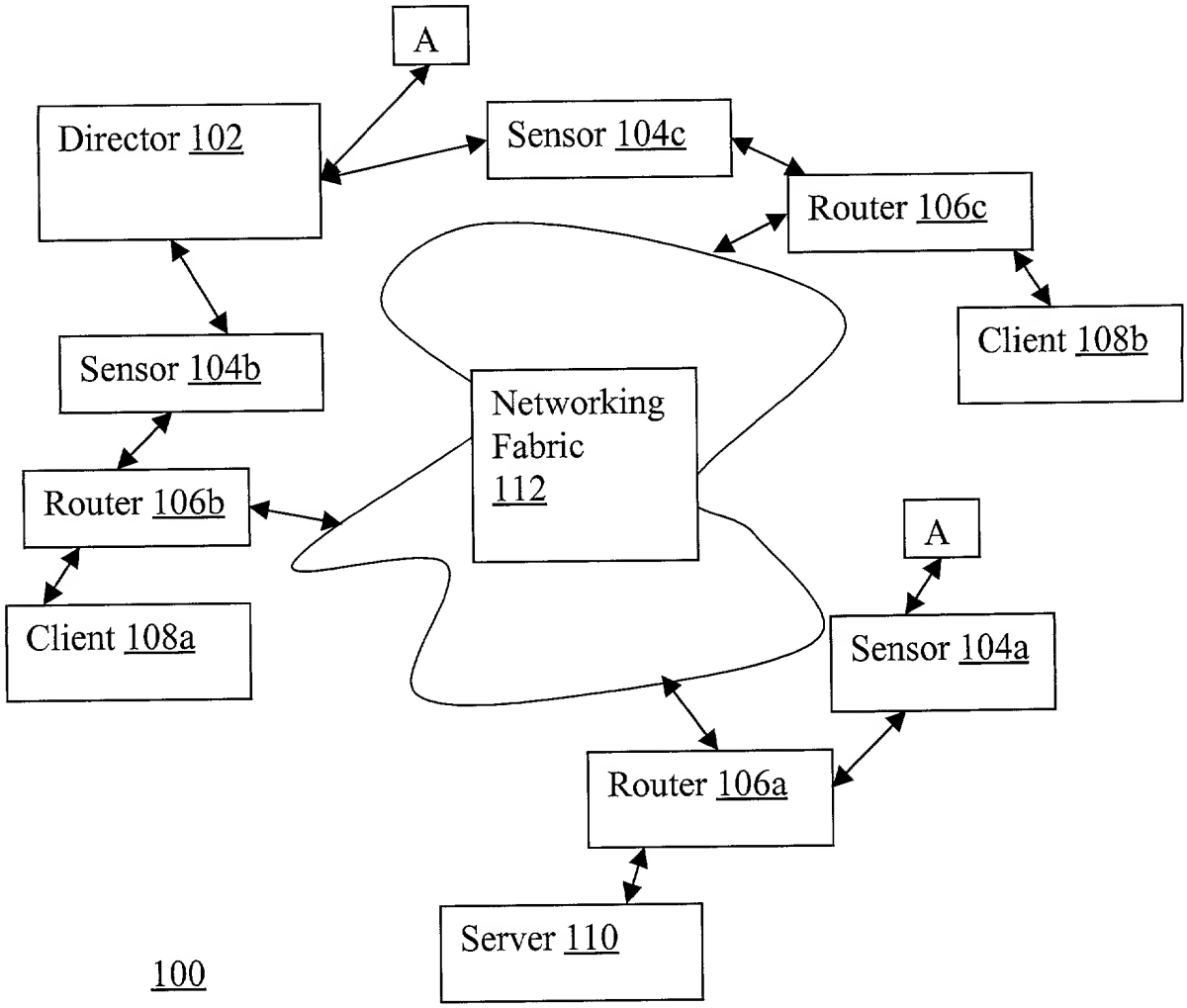
A
Director 102
Sensor 104c
Router 106c
Client 108b
Sensor 104b
Networking
Fabric
112
Router 106b
Client 108a
A
Sensor 104a
Router 106a
Server 110
100

Figure 1

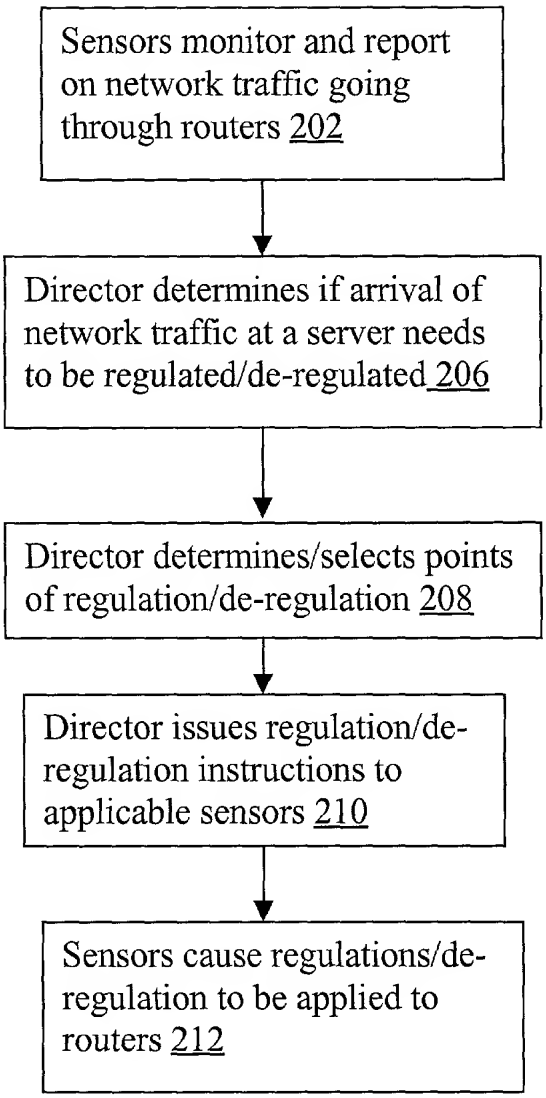
Sensors monitor and report on network traffic going through routers 202
Director determines if arrival of network traffic at a server needs to be regulated/de-regulated 206
Director determines/selects points of regulation/de-regulation 208
Director issues regulation/de-regulation instructions to applicable sensors 210
Sensors cause regulations/de-regulation to be applied to routers 212
200

Figure 2

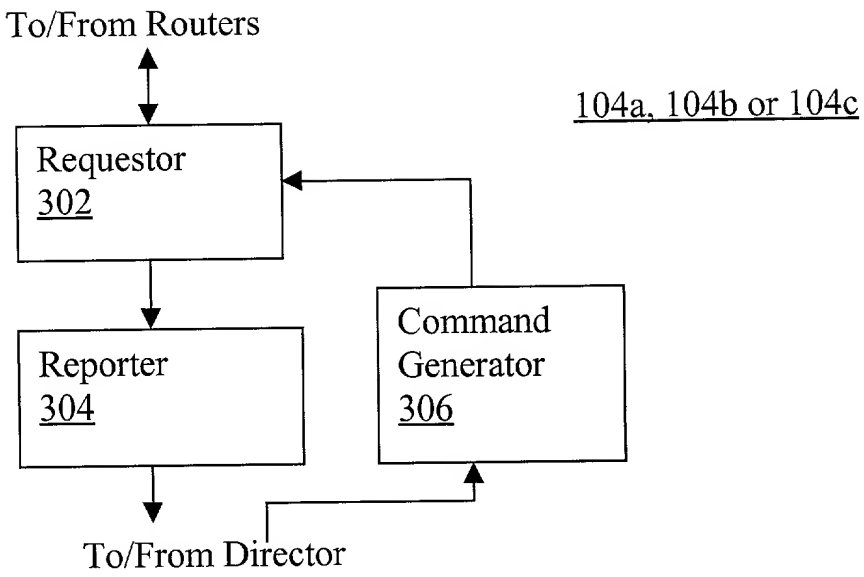
To/From Routers
104a, 104b or 104c
Requestor
302
Reporter
304
Command
Generator
306
To/From Director

Figure 3

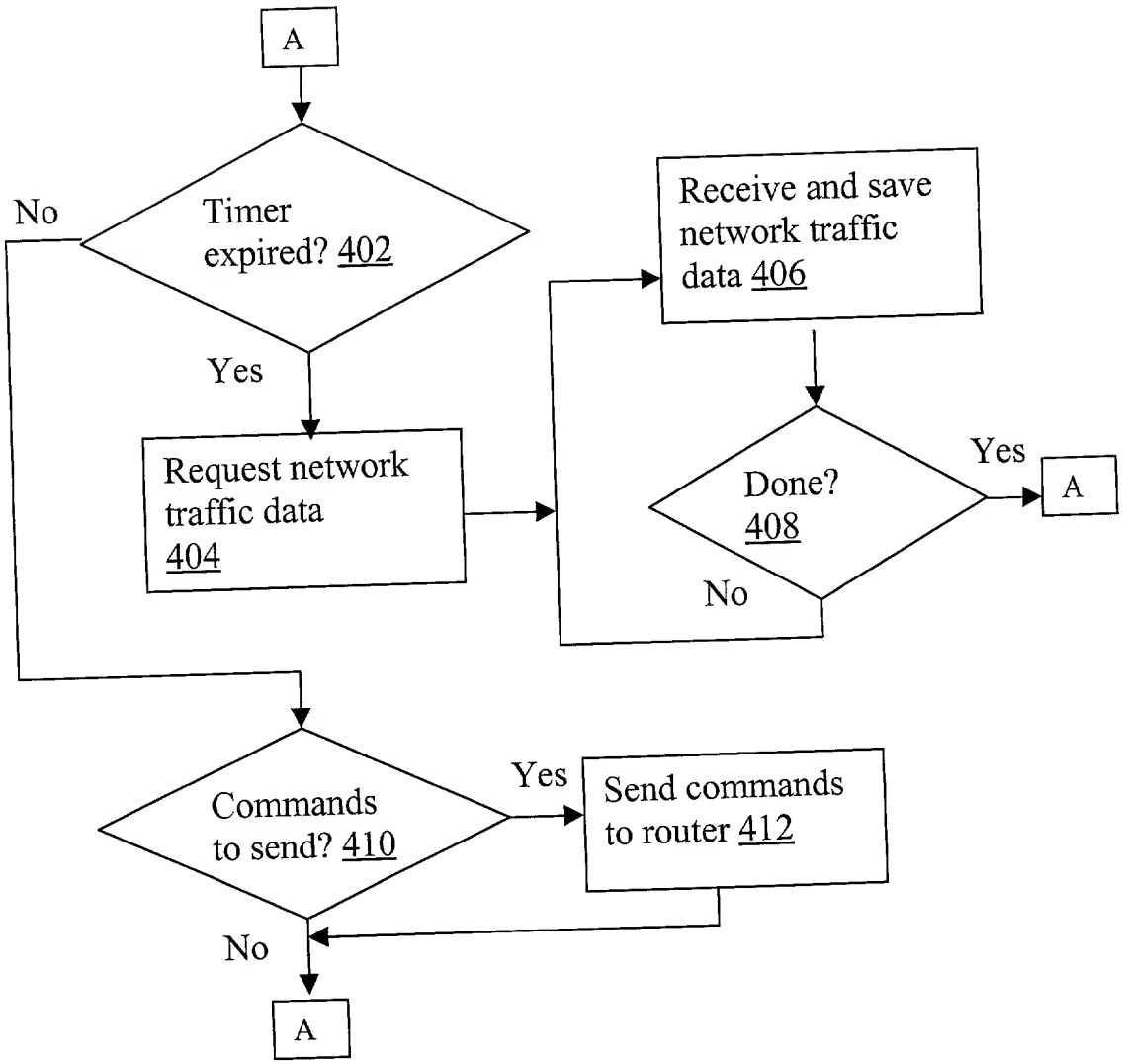
A
Timer expired? 402
No
Yes
Request network traffic data 404
Receive and save network traffic data 406
Done? 408
Yes
A
No
Commands to send? 410
Yes
Send commands to router 412
No
A

Figure 4

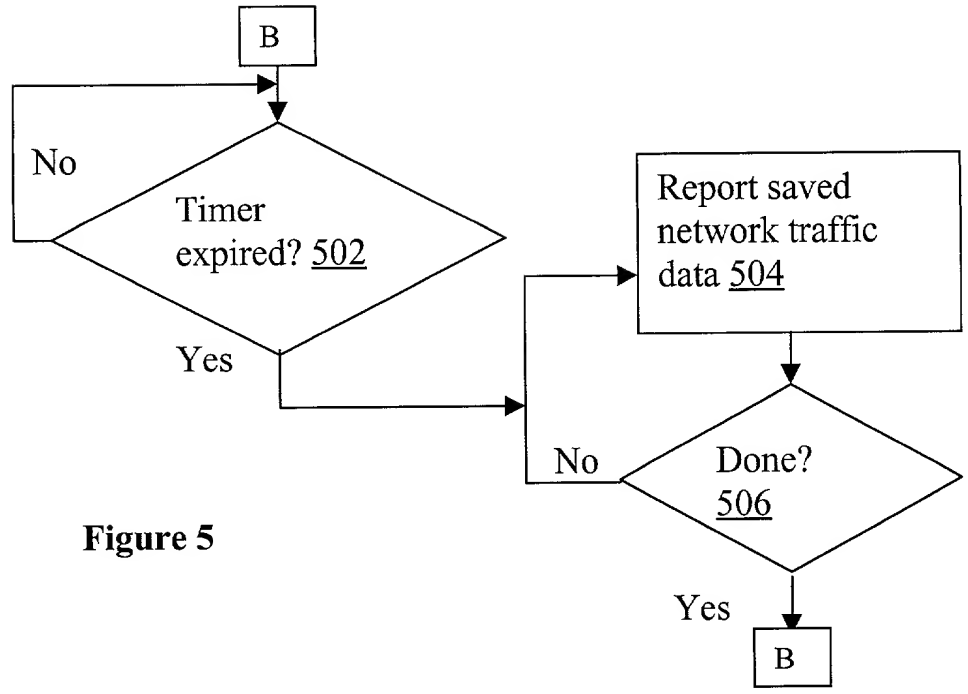

Figure 5

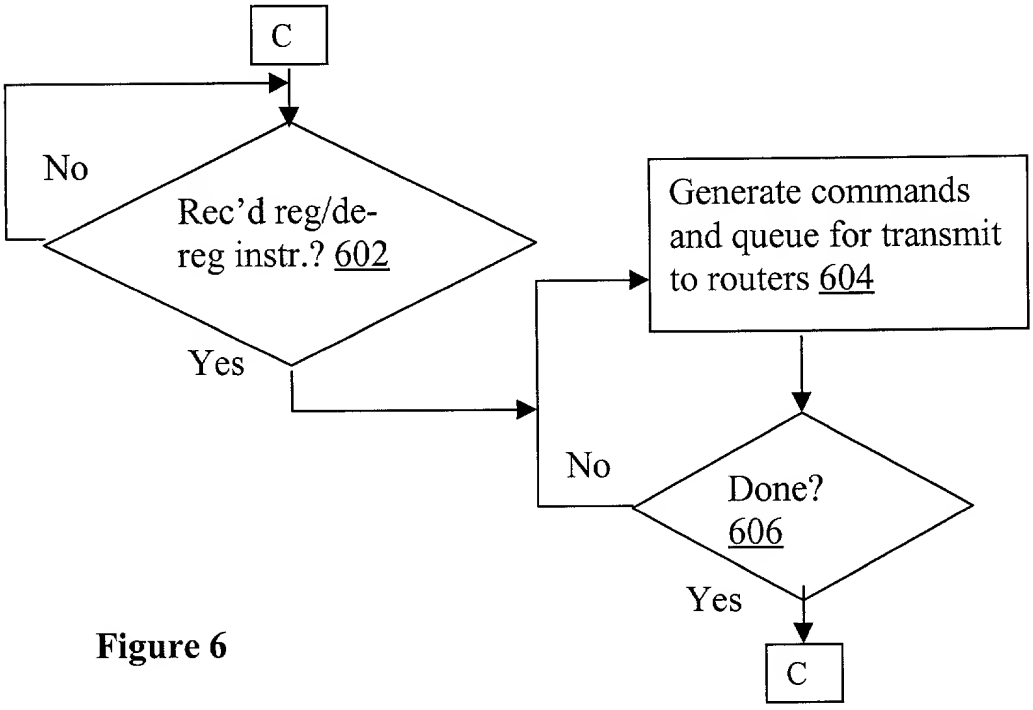

Figure 6

700

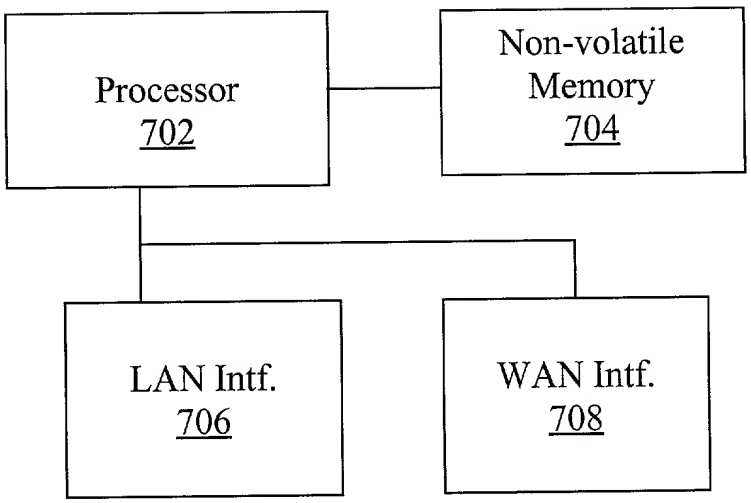
Processor
702
Non-volatile
Memory
704
LAN Intf.
706
WAN Intf.
708

Figure 7

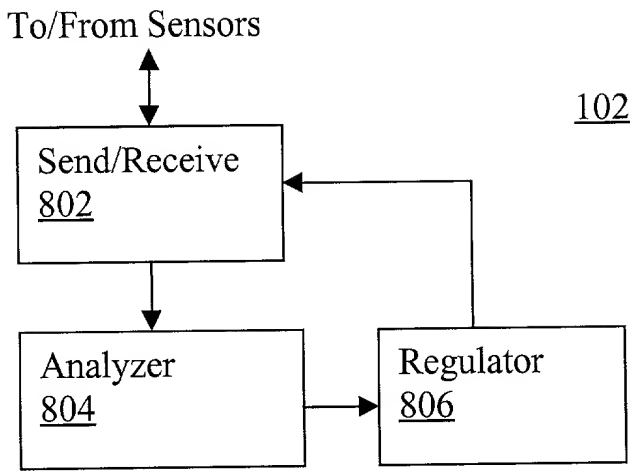

Figure 8

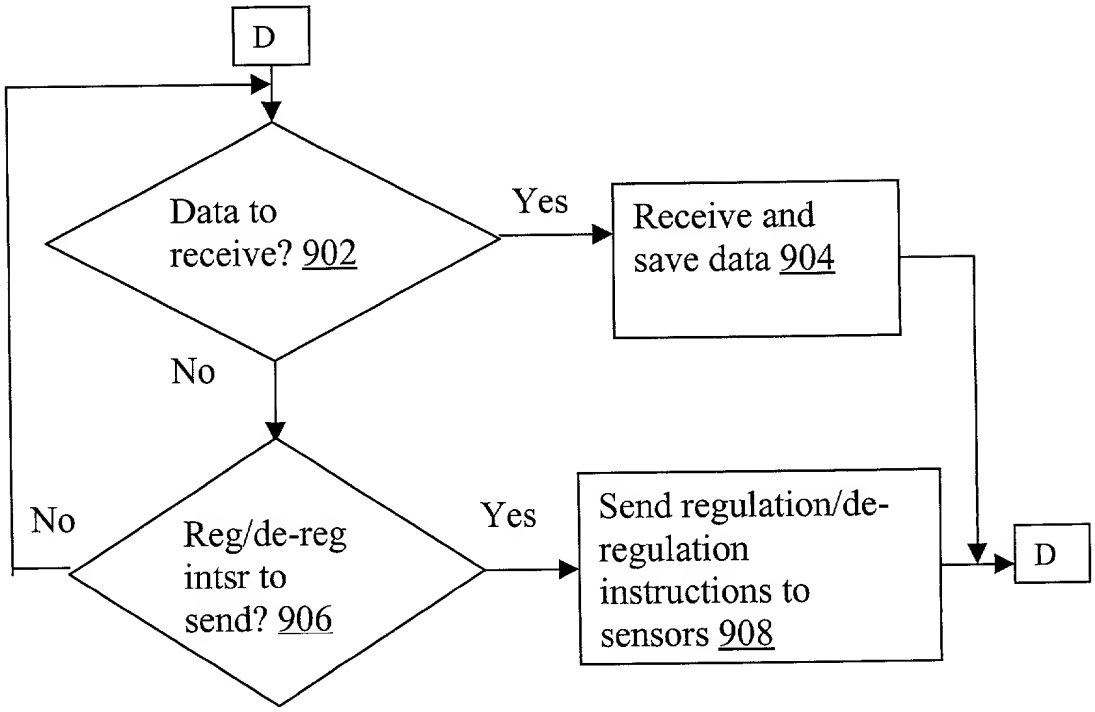

Figure 9

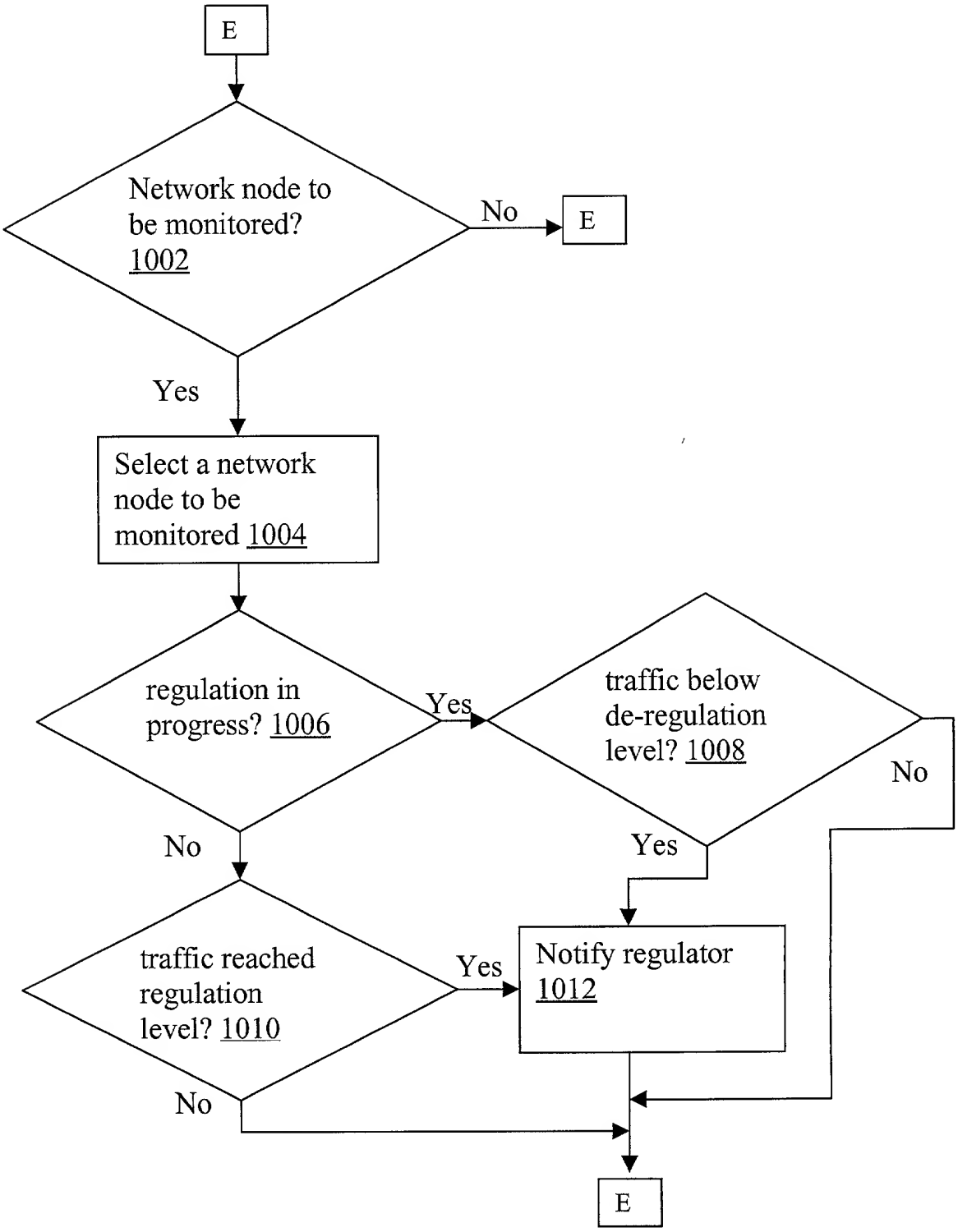
E
Network node to be monitored? 1002
No
E
Yes
Select a network node to be monitored 1004
regulation in progress? 1006
Yes
traffic below de-regulation level? 1008
No
Yes
No
traffic reached regulation level? 1010
Yes
Notify regulator 1012
No
E

Figure 10

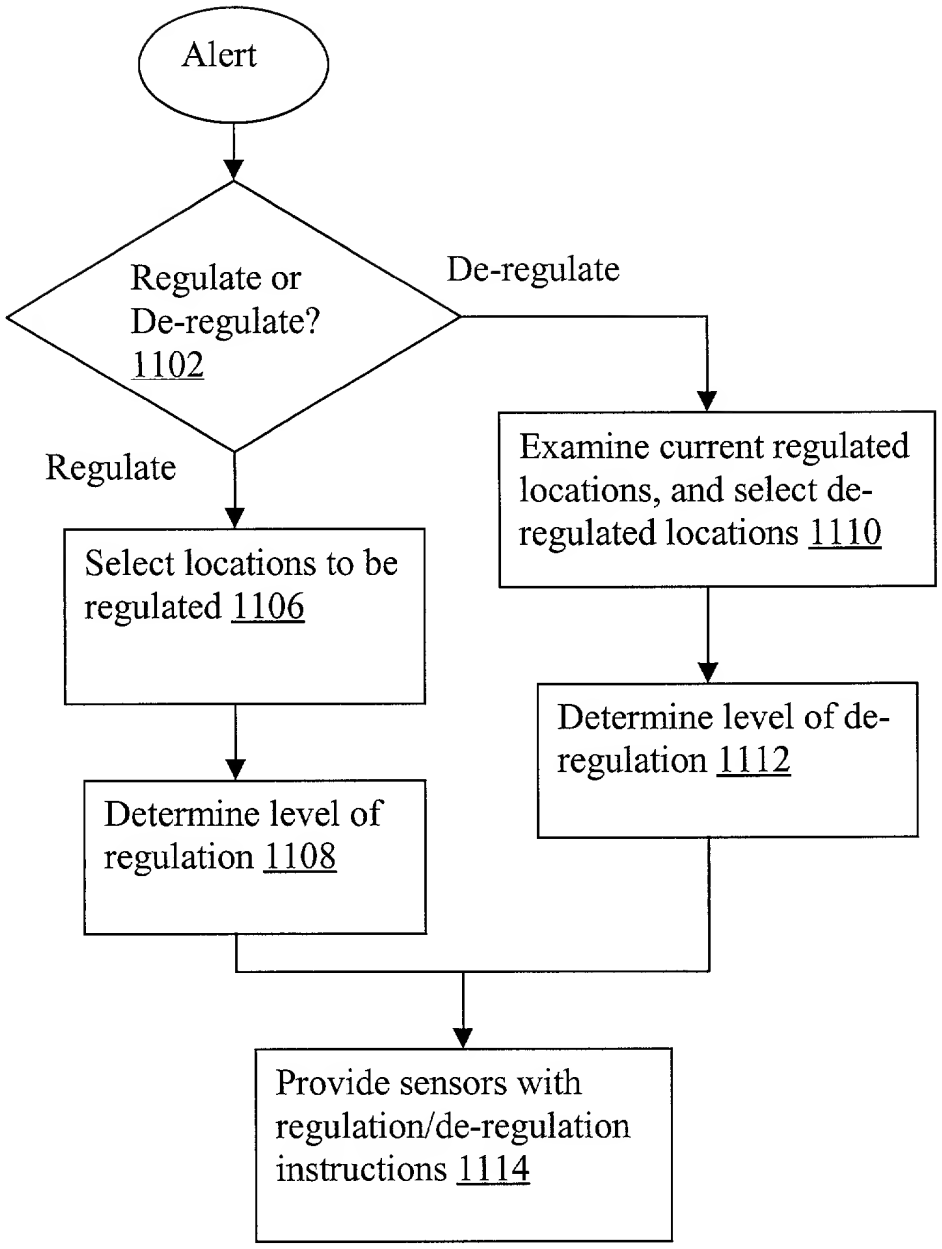
Alert
Regulate or De-regulate? 1102
De-regulate
Regulate
Examine current regulated locations, and select de-regulated locations 1110
Select locations to be regulated 1106
Determine level of de-regulation 1112
Determine level of regulation 1108
Provide sensors with regulation/de-regulation instructions 1114

Figure 11

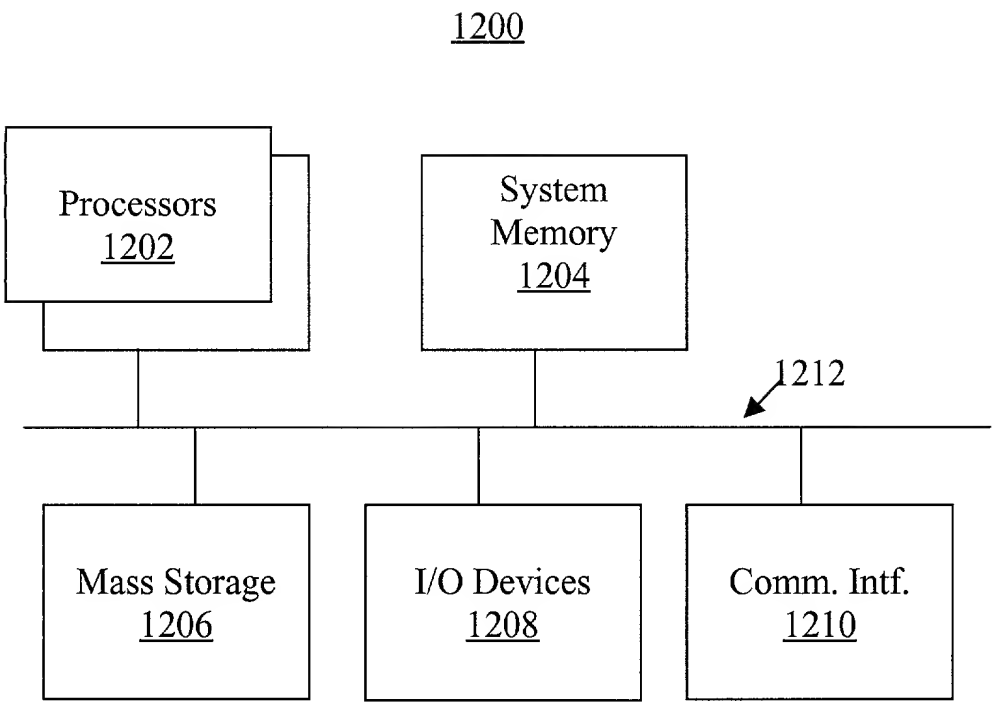
1200
Processors
1202
System
Memory
1204
1212
Mass Storage
1206
I/O Devices
1208
Comm. Intf.
1210

Figure 12

Attorney's Docket No.: 05129.P001 Patent

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
A DISTRIBUTED SOLUTION FOR REGULATING NETWORK TRAFFIC

the specification of which

__X__ is attached hereto.
___ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Aloysius T.C. AuYeung (Name of Attorney or Agent), BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to Aloysius T.C. AuYeung (Name of Attorney or Agent), (425) 827-8600.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor David J. Wetherall

Inventor's Signature ______________ Date Aug 4, 2000

Residence Seattle, WA (City, State) Citizenship Australia (Country)

Post Office Address 301 Summit Avenue East, Apt. 302
Seattle, WA 98102

Full Name of Second/Joint Inventor Thomas E. Anderson

Inventor's Signature ______________ Date Aug 4, 2000

Residence Seattle, WA (City, State) Citizenship USA (Country)

Post Office Address 1201 18th Avenue East
Seattle, WA 98112

Full Name of Third/Joint Inventor Stefan R. Savage

Inventor's Signature ______________ Date 8/4/2000

Residence Seattle, WA (City, State) Citizenship USA (Country)

Post Office Address 4137 SW Portland Street
Seattle, WA 98136

Full Name of Fourth/Joint Inventor ______________

Inventor's Signature ______________ Date ______________

Residence ______________ (City, State) Citizenship ______________ (Country)

Post Office Address ______________

Full Name of Fifth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

Full Name of Sixth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

Full Name of Seventh/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. 44,587; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Alin Corie, Reg. No. P46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Kurt P. Leyendecker, Reg. No. 42,799; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. 44,976; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Marina Portnova, Reg. No. P45,750; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; James M. Wu, Reg. No. 45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Justin M. Dillon, Reg. No. 42,486; my patent agent, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.